EP 22975 3

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 844 767 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.05.1998 Bulletin 1998/22

(51) Int. Cl.[6]: **H04L 29/06**

(21) Application number: **97306102.1**

(22) Date of filing: **11.08.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **19.11.1996 US 752421**

(71) Applicant:
NCR INTERNATIONAL INC.
Dayton, Ohio 45479 (US)

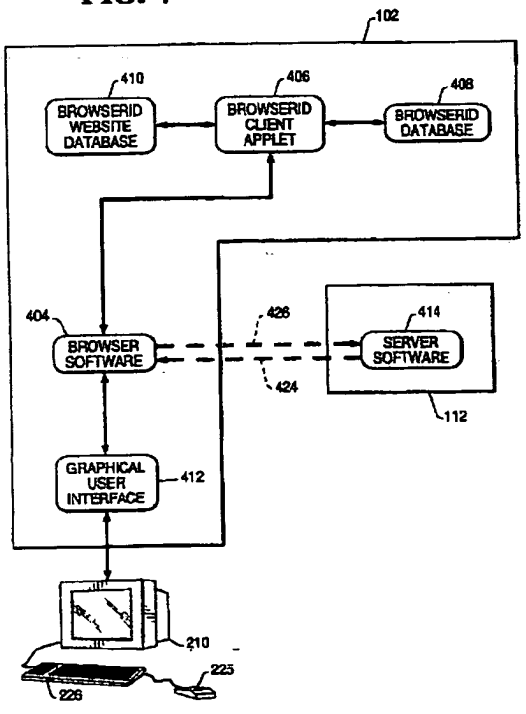
(72) Inventors:
- **Rowland, Bruce R.**
  St. Charles, IL 60174 (US)
- **Friedman, Lee G.**
  Alpharetta, BA 30202 (US)

(74) Representative:
Irish, Vivien Elizabeth
International IP Department,
NCR Limited,
206 Marylebone Road
London NW1 6LY (GB)

(54) User controlled browser

(57) A mechanism provides a user-controlled information disclosure process. A user information database (206,208), a BrowserID Client applet (406), and a BrowserID Website database (408) are configured at a user terminal (102). The user information database contains a plurality of information records about a user's identification information and access levels for the respective information records. The BrowserID Website database contains the names of web sites and access levels for the respective web sites. In response to a request for user information from a web site, the BrowserID Client applet checks the existing access level in the BrowserID Website database for the web site (or negotiates a new level), and if appropriate, retrieves the access key granted by the web site to gain access to a controlled portion of a website.

FIG. 4



EP 0 844 767 A1

Printed by Xerox (UK) Business Services
2.16.3/3.4

Description

The present invention relates to a method and apparatus for providing user identification and transaction information to web sites in the process of getting access to the web sites.

It is known a user can retrieve information from world wide web sites (or web sites) via the Internet. More specifically, in retrieving desired information from a particular web site, the user sends a service request to the web site by using the web browser software at a user terminal. Upon receiving the service request, server software for the web site searches the information repository (organized as web pages) in the web site according to the request, and sends the desired information to the user terminal. Upon receiving the desired information, the web browser software displays the desired information in page format to the user.

To enhance the quality of, expand the market for, and provide new services for their web site services, many web sites require visitor identification and ask for personal identification and demographic information before processing received service requests. Further, the user may be required to provide a credit card or other sensitive financial information The user identification can be useful for a number of purposes: to authenticate web visitors, to selectively grant access privileges, to facilitate the administration and billing of marketable services over the Internet, to provide more focused responses, to build customer history database to facilitate the consequent repeating services, to collect marketing information, etc.

At the present time, several approaches have been developed to gather user identification information. One approach, used by Netscape Inc., is to "quietly" maintain a file within the client accessible to the browser software at user terminals. When a user terminal sends a service request to a web site, the browser software first provides to the server software the information within the file (known as "cookies.txt") that applies to the server's domain (Internet address). One problem with this approach is that users have little control (short of deleting the file or its entries), regardless of what types of web sites they are visiting. Another problem with this approach is that the user identification may be incomplete, because the user identification gathered is limited to the hardware and software configuration at the user terminal. Current tracking facilities identify a web visitor by recognizing a unique identifier associated with the web visitor based on exchanges between the browser software and the server software. Usually, the identifier is the IP (Internet Protocol) address of the user terminal the visitor is using. This type of identification is problematic since many on-line service providers (such as American Online and CompuServe) assign an IP address per user session and will re-use the IP address for other users when it is released. It is also possible that corporate proxy servers hide (or mask) individual IP addresses for associated user terminals with their firewalls.

In another approach, many web sites have implemented a registration facility. After sending a service request to a web site, an HTML (Hyper Text Markup Language) form is presented to the web visitor, requesting the visitor to fill in the form to provide information such as name, e-mail address, phone number, business affiliation, etc. Often the registration is accompanied by the issuance of personal ID and password for use in the next visit to the web site, typically giving the visitor access to pages of information and services not otherwise available. Such a registration process is cumbersome and inconvenient for a web site user. The format of the identification information is designed to satisfy each individual web site and may be not consistent to the user. It is quite possible the information being requested is not handy at the moment when the user is visiting a web site. If multiple personal IDs and pass words are issued, it is difficult for the user to remember the IDs and passwords and match them with appropriate web sites.

To strike a balance between the users' privacy and the necessity to have user identification information, Daniel W. Connolly made two proposals in July of 1995 ("Request-ID header field" and "Anonymous Authentication"). These two proposals focus on per session tracking and thus are not amenable to establishing a long term relationship between a web side provider and customer, or to providing insight to users identification for demographic purposes. A third proposal by Daniel W. Connolly suggests establishing an "electronic business card" through the use of HTML forms and ID field names that would facilitate the filling in of common registration forms by having standardized field names that could automatically be filed by a browser. The browser user would have the opportunity not to submit the information or to edit it prior to submitting it. A problem with this proposal is the negative impact that it would have on caching performed by proxy servers since the ID information would be transmitted via URLs (Uniform Resource Locators) that are the keys to cached web pages.

Therefore, there exists a need to provide a method and apparatus that can provide user identification information to web sites under users' control.

There exists another need to provide a method and apparatus that can provide user identification information to web sites with control, consistency, efficiency, and convenience to the users.

The object of the present invention is to meet these needs.

According to the invention a method for providing information to a web site at a user terminal, characterized by the steps of:

at the user terminal,

(a) establishing a plurality of information records with respective access level indicators for indicating access levels;

(b) receiving a request from the web site with an access level being associated with the web site;

(c) checking the access level for the web site; and

(d) retrieving information records based on said access level indicators associated with the information records and the access level associated with the web site.

Also according to the invention an apparatus for providing information to a web site at a user terminal, characterized by the user terminal comprising

a receiver circuit for receiving a request from the web site with an access level being associated with the web site; and

a processor logic for checking the access level for the web site; and for retrieving information based on the access level associated with the web site.

The invention will be described by way of example with reference to the appended drawings, in which:

Figure 1 shows an exemplary data network configuration;

Figure 2 shows a hardware block diagram of a representative one of the user terminals of Figure 1;

Figure 3 shows a hardware block diagram for a computer system, which is able to support any one of the web sites of Figure 1;

Figure 4 shows a software block diagram for a representative one of the user terminals, and for a representative one of the web sites, shown in Figure 1;

Figure 5 shows BrowserID database of Figure 4 in greater detail;

Figure 6 shows BrowserID website database of Figure 4 in greater detail; and

Figure 7 shows a flowchart illustrating the steps of disclosing user information to a web site.

Referring to Figure 1, there is shown an exemplary data network configuration 100, which includes a plurality of user terminals ($102._1$, $102._2$, ..., $102._M$), a plurality of web sites ($112._1$, $112._2$, ..., $112._N$), and a data network 106. Each of the user terminals can get access to the web sites via data network 106.

As shown in Figure 2, a user terminal 200 comprises a processing unit 202, a memory device 204, a disk drive interface 208, a display interface 212, a serial interface 224, and a network communication interface 234, all connected to a system bus 214.

A hard disk 206 is coupled to the disk drive interface 208; a display monitor 210 is coupled to the display interface 212; and a mouse 225 and a keyboard 226 are coupled to the serial interface 224.

Memory device 204 and the hard disk 206 are both able to store programs. However, memory device 204 has faster access speed than hard disk 206, while hard disk 206 has higher capacity than memory device 204.

Network communication interface 234 is able to provide an interface between the user terminal and data network 106. More specifically, all software function blocks as shown in figures 2 and 3 get access to data network 106 via network communication interface 234 in compliance with pre-determined network protocols.

The processing unit 202 is able to control operations of a user terminal by executing programs stored in memory device 204 or hard disk 206. Processing unit 202 is also able to control the transmissions of programs and data between memory device 204 and hard disk 206.

Referring to Figure 3, there is shown a hardware block diagram for a computer system 300, which is able to support any of the web sites ($112._1$, $112._2$, ..., $112._N$), and comprises a processing unit 302, a memory device 304, a disk drive interface 308,and a network communication interface 334, all connected to a system bus 314. The disk drive interface 308 is coupled to a hard disc 306.

Memory device 304 the hard disk 306 are both able to store programs. However, memory device 304 has faster access speed than hard disk 306, while hard disk 306 has higher capacity than memory device 304.

Network communication interface 334 is able to provide an interface between computer 300 and data network 106 in compliance with pre-determined network protocols.

Processing unit 302 is able to control operations of computer system 300 by executing programs stored in memory device 304 or hard disk 306, and is also able to control the transmissions of programs and data between memory device 304 and hard disk 306.

In Figure 4, a user terminal includes five software function blocks 404 to 414.

Browser software 404 is able to formulate and send requests to web sites, and to display the information retrieved from the web sites. Browser software is also able to receive user ID information requests from web sites.

BrowserID database 408 contains user information.

BrowserID client applet 406 is able to retrieve the user information from BrowserID database 408 and passes it to browser software 404. However, BrowserID client applet 406 will not pass any user information from BrowserID database 408 without the explicit permissions the user set in the BrowserID database 408 and comparing them to the defined set of permissions in the BrowserID website database 410 for that web site 414. If, in response to a request for user ID information from a web site, no permission is granted to the web site, the browser software 404 will alert the user to define a permission that will be entered into the BrowserID website

database 410. BrowserID client applet 406 is designed (programmed in Java for example) such that it can be executed (or interpreted) by any browser.

BrowserID website database 410 contains the names of web sites and the degree of identification information to be shared.

Graphical User Interface 412 is able to provide an interface between a user and software function blocks, including BrowserID client applet 406 and BrowserID database 408. Through display monitor 210, keyboard 225 and mouse 226, a user is able to initialize and update the BrowserID database 408_and the BrowserID website database 410, and to send control signals to BrowserID client applet 406.

Server software 414 is able to process the requests for information from browsers and return the information to the browsers via HTTP, FTP, Gopher or other Internet information transfer protocols.

When a user wants to visit web site 112, he/she can use keyboard 225 or mouse 226 to activate browser software 404 to send a service request to the web site, as indicated by line 426. Upon receiving the service request, server software 414 for the web site sends a request for user ID information, as indicated by line 424 which will invoke the execution on the user terminal of Browser ID Client Applet 406.

Figure 5 shows BrowserID information database 408 which contains rows of ID records, each with two fields, namely: a single ID Information Item followed by an information sharing Level Limit field. In the first record, the ID Information Item field contains a user's full name; the Level Limit field contains a numerical value, indicating that the name will be revealed to a web server of a web site if and only if the user chooses to provide that level of information access for that web server. If so, that sharing level will be indicated within the BrowserID website database 410 by the Level Limit Field. By way of another example, in the seventh record, the ID Information Item field contains social security number; the Level Indicator Field contains 7, indicating that the social security number will only be transmitted to the web server of a web site if and only if the user specifies a web server's access level within the BrowserID website database 410 of value 7 or higher.

In the embodiment shown in Figure 5, it is assumed that the greater the numerical value in the Level Limit field, the higher is the access level. It can be designed the other way around, that is: the smaller of the numerical value in the Level Limit field, the higher is the access level. This means that a record will be revealed to a web server of a web site if and only if the web server's access level from the BrowserID website database 410 is smaller than or equal to the Level Limit Field associated to that record.

As shown in Figure 6, BrowserID website database 410 is comprised of records with 2 fields. The first field is the public URL for the site. The second field contains the access level assigned to it by the user when information sharing level access was negotiated among the BrowserID Client Applet and the web site server. This information is stored in the BrowserID website database 410 and is indexed by the BrowserID database 408 under control of the BrowserID applet 406.

Figure 7 illustrates the steps of disclosing user information to a web site.

In step 704, a user sends a service request to one of the web sites ($112._1$, $112._2$, ..., $112._N$), that requires access from one of the user terminals ($102._1$, $102._2$, ..., $102._M$), to request an access to the web site.

In step 706, server software 414 for the web site returns the web site name that will provide the service requested by the user and a request for information to BrowserID Client applet 406. In its request, the server software (414) may specify the information items it needs, such as name, address, phone number, ..., etc.

In step 707, BrowserID Client applet 406 determines whether an entry exists for the returned web site name in the BrowserID Website database 410. If an entry exists for the returned web site name, the operation is led to step 710. If no entry exists for the returned web site name, the operation is led to step 708.

In step 708, to negotiate a Level Limit to share information with the web site, BrowserID Client applet 406 presents an HTML form, including the information items specified by sever software 414, to the user.

Following step 708, in step 709, BrowserID Client Applet 406 creates an entry in BrowserID database 408 for the returned web site name, and the user selects a Level Limit, in reference to the HTML form. The user may choose to the Level Limit that complies with the information items specified by the web site, or choose to grant a lower Level Limit. The operation is then led to step 710.

In step 710, BrowserID Client applet 406 determines whether any of the information items specified by the web site exceed the Level Limit previously granted to the web site, by using the information stored in BrowserID database 408 and BrowserID website database 410.

In step 710, if the Level Limit previously granted is not exceeded, the operation is led to step 712. If the Level Limit is exceeded, the operation is led to step 711, in which BrowserID Client applet 406 presents an HTML form to the user, asking the user to permit the increase in the Level Limit to the web site and asking if the user wants this to be a permanent update. After the user responds (either increases the Level Limit, or keeps the Level Limit previously granted unchanged), the operation is then led to step 712.

In step 712, BrowserID Client applet 406 responds to the server software with the information fields from BrowserID database 408, according to the Level Limit granted to the web site.

In step 722, server software 414 processes the requests from browser software 404, to proceed with web site activity.

Preferably, in the embodiment shown in figures 2 and 4, the software function blocks for a user terminal are stored in memory device 204 or hard disk 206 and executed by processing unit 202. In the embodiment shown in figure 3, server software is stored in memory 304 and executed by processing unit 302.

It should be appreciated that the present invention provides a mechanism for users to control their own identification information. As such, the present invention requires that the BrowserID Client Applet which collects and delivers user information for web sites must be permanently associated with the client's browser; an applet that is downloaded from a website server cannot be trusted to cooperate with the user's desire to control access to personal information.

The present invention has the advantages in that:

(a) a user can control ID information disclosure at different level; (b) it is convenient for a user to provide the ID information; (c) it creates a mechanism to provide a standardized mechanism and format to provide ID information; and (d) web servers get complete and accurate ID information (if disclosed).

Claims

1. A method for providing information to a web site at a user terminal, characterized by the steps of:

   at the user terminal,

   (a) establishing a plurality of information records with respective access level indicators for indicating access levels;
   (b) receiving a request (706) from the web site with an access level being associated with the web site;
   (c) checking (707,710) the access level for the web site; and
   (d) retrieving (712) information records based on said access level indicators associated with the information records and the access level associated with the web site.

2. A method according to claim 1, in which in step (a) the access level associated with the web site is defined by the user terminal.

3. A method according to claim 1 or claim 2 further comprising establishing a plurality of first type of records containing access levels associated with the web sites and establishing a plurality of second type of records, each one of said second type of records containing user information and access level associated with said one record;

   and on receiving a request from one of the web sites checking access level for the web site from said first type of records, and retrieving information from said second type of records based on the access level associated with the web site and the access levels associated with said second type of records.

4. An apparatus for providing information to a web site at a user terminal, characterized by the user terminal comprising

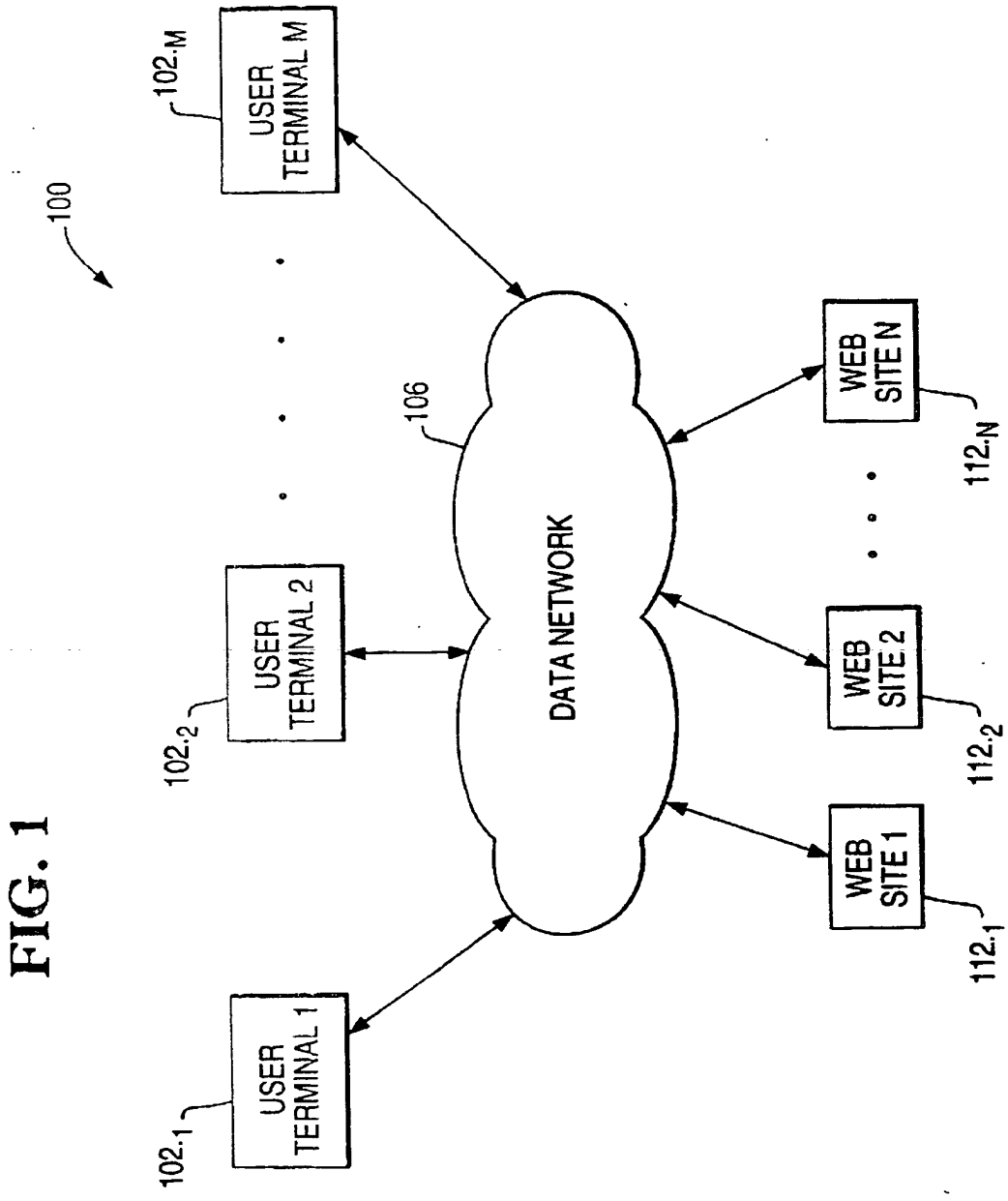
   a receiver circuit for receiving a request from the web site with an access level being associated with the web site; and
   a processor logic for checking the access level for the web site; and for retrieving information based on the access level associated with the web site.

5. An apparatus according to claim 4 further comprising:

   a storage medium for storing a plurality of information records with respective access level indicators for indicating access levels, and arranged so that the processor logic retrieves information records based on said access level indicators associated with the information records and the access level associated with the web site.

6. A apparatus according to claim 5 in which said access level indicators are definable at the user terminal.

FIG. 1



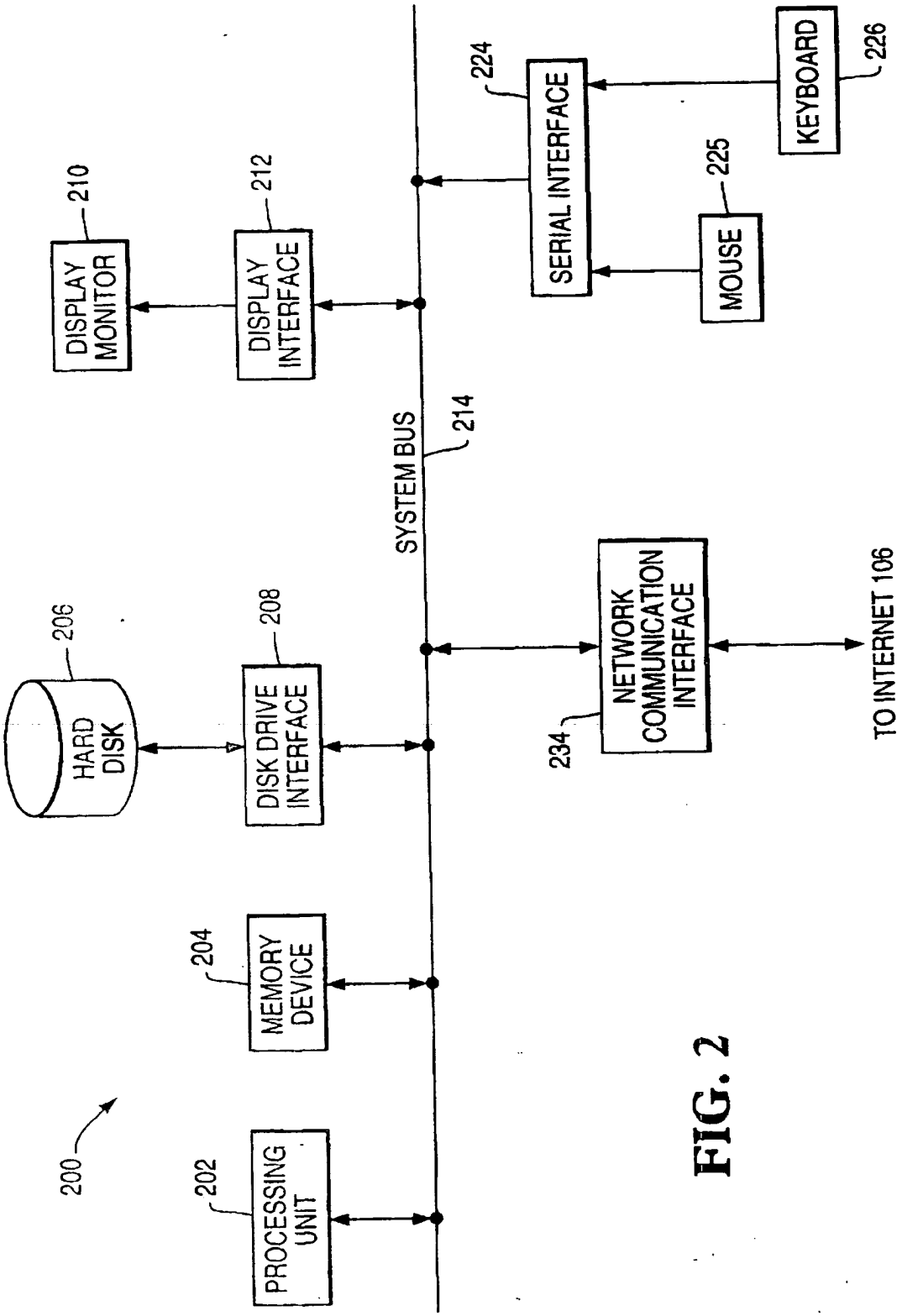


FIG. 2

FIG. 3

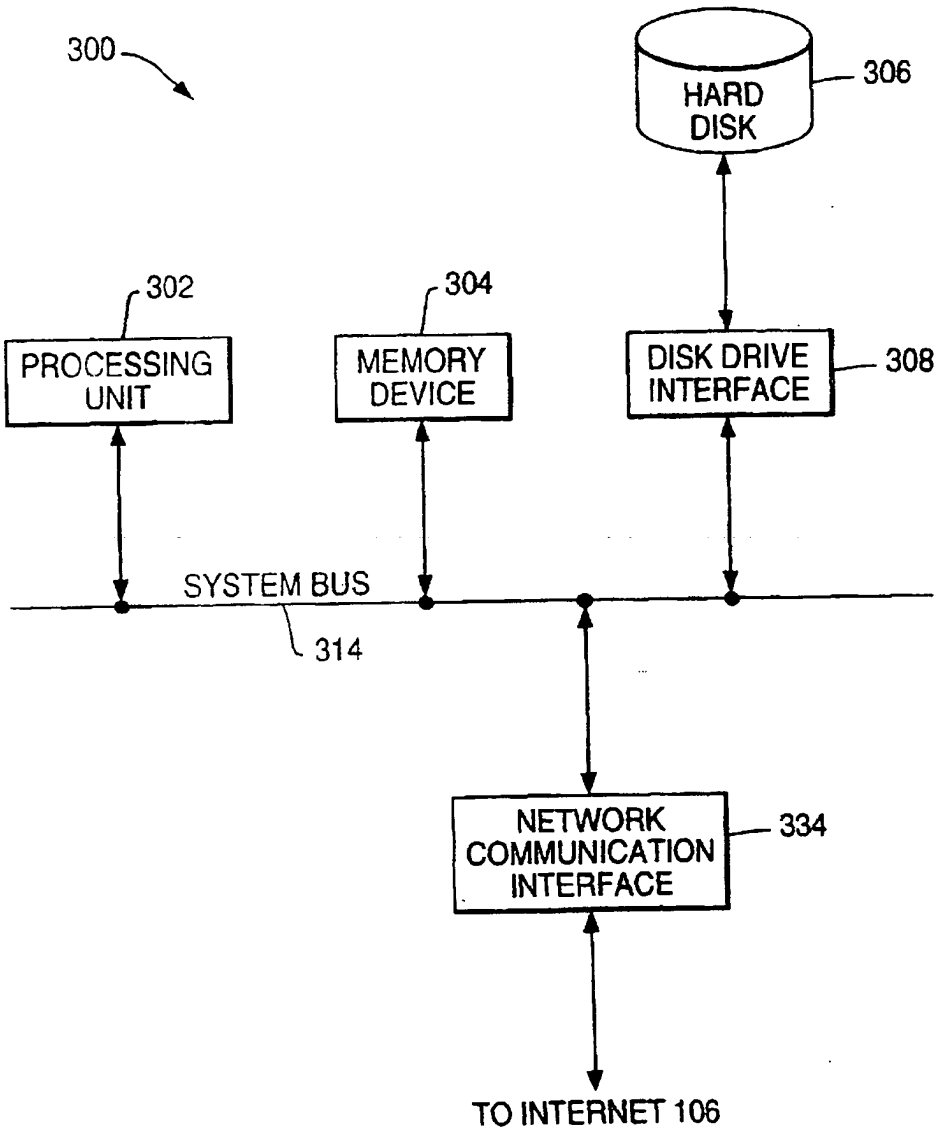


FIG. 4

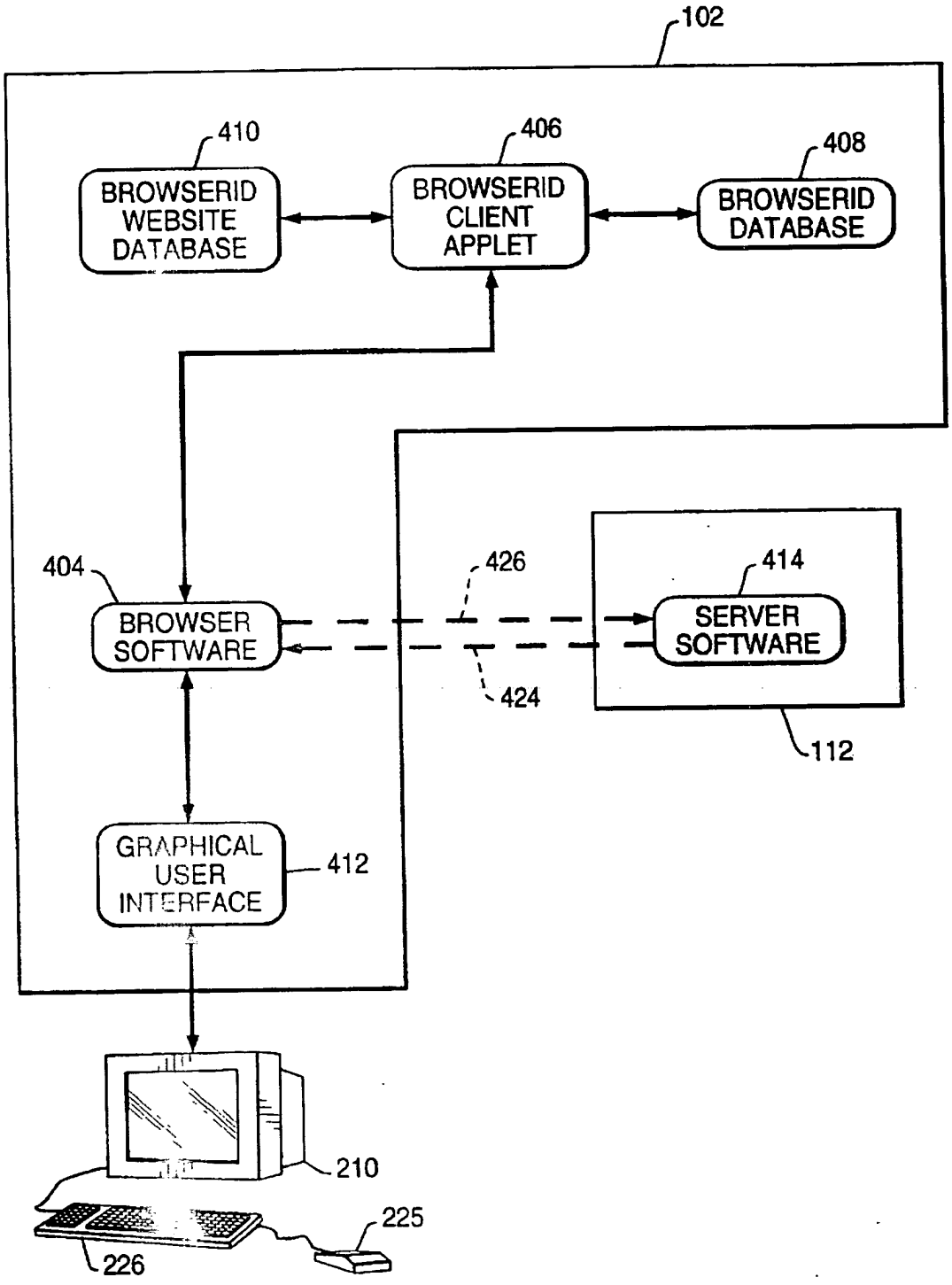


FIG. 5

BROWSERID DATABASE

ID INFORMATION ITEM	LEVEL LIMIT
NAME	1
ADDRESS	4
PHONE	4
FAX	4
E – MAIL	2
DEMOGRAPHICS	5
SOCIAL SECURITY NO.	7
BANK ACCOUNT NO.	9
CREDIT CARD	9
MOTHER'S MAIDEN NAME	8
SOFTWARE SERIAL NO.	7
USER NAME	10
PASSWORD	100

FIG. 6

BROWSERID WEBSITE DATABASE

WEBSITE	ACCESS LEVEL
WWW.MICROSOFT.COM	2
WWW.WALMART.COM	3
WWW.SOFTWARE.NET	5
WEBSITE NAME	3
WEBSITE NAME	5
WEBSITE NAME	6
WEBSITE NAME	M
WEBSITE NAME	M + 2
WEBSITE NAME	N

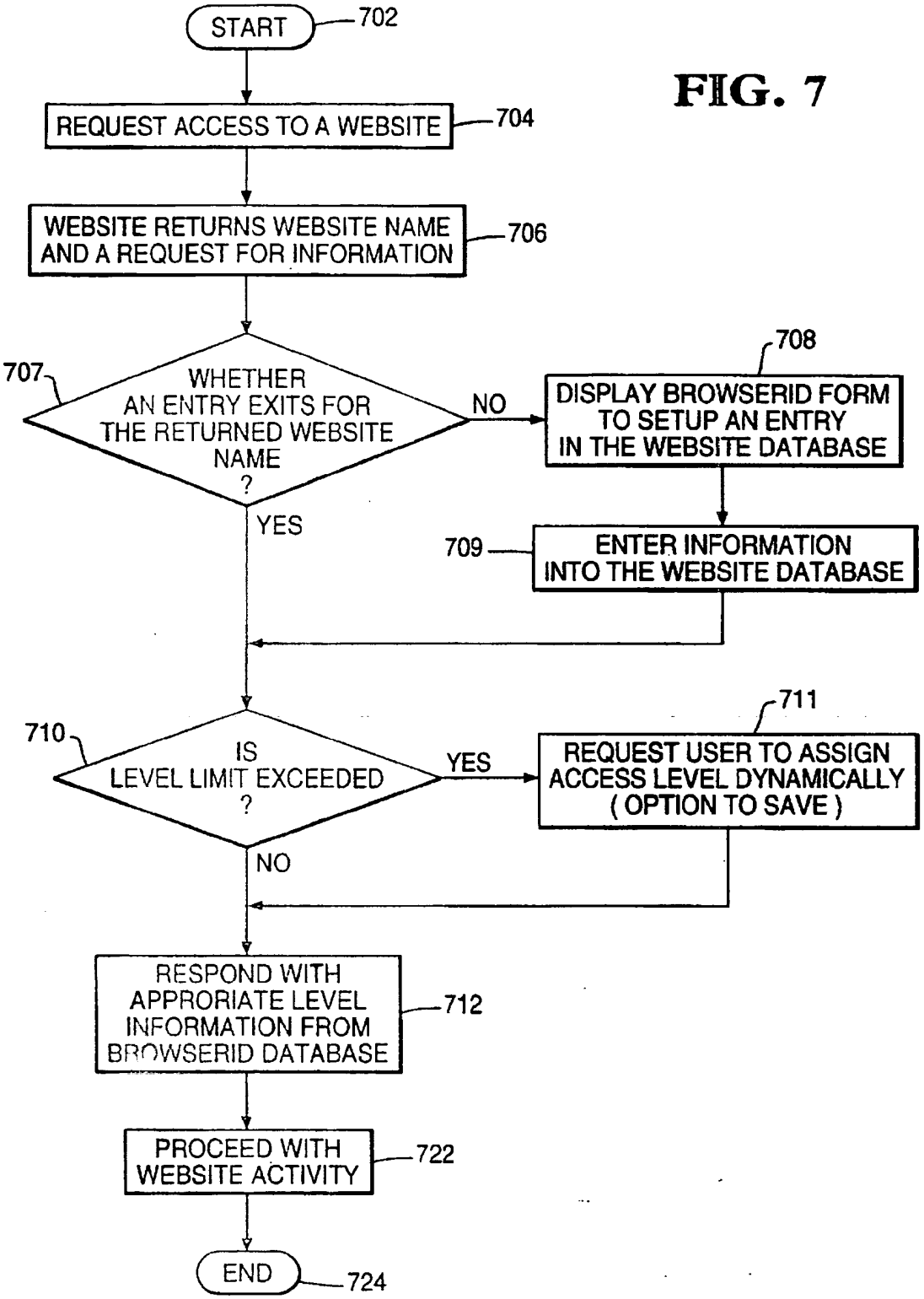


FIG. 7

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 30 6102

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	BRANDS S: "ELECTRONIC CASH ON THE INTERNET" PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, 1 January 1995, pages 64-84, XP000567597 * paragraph 1 - paragraph 3 * * paragraph 9 * * figure 1 * ---	1-6	H04L29/06
Y	GHANI D: "CHARGING AND PAYING FOR INFORMATION ON OPEN NETWORKS" ASLIB PROCEEDINGS, vol. 47, no. 6, 1 June 1995, pages 145-148, 151/152, XP000578745 * paragraph 4 - paragraph 5 * ---	1-6	
A	MAAREK Y S ET AL: "Automatically organizing bookmarks per contents" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 11, no. 28, May 1996, page 1321-1333 XP004018230 * paragraph 1 - paragraph 3 * -----	1-6	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	13 March 1998	Poggio, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)